U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Summary of Audit Report

National Nuclear Security Administration's Use of Innovative Technologies to Meet Security Requirements

This document provides a summary of an Audit Report that is not publicly releasable. Public release is controlled pursuant to the Freedom of Information Act

OAS-L-09-02 October 2008

The following is a summary of a Special Access Unclassified Controlled Nuclear Information Audit Report, OAS-L-09-02, dated October 31, 2008, entitled "National Nuclear Security Administration's Use of Innovative Technologies to Meet Security Requirements. The complete report is not available for public disclosure.

BACKGROUND

The Department of Energy (Department) developed the Design Basis Threat policy (DBT), which identified the most credible threats posed by potential adversaries to Departmental assets and operations. Since the terrorist attacks of September 2001, revisions to the DBT have established significantly more stringent standards for protecting Departmental assets and operations. The DBT provides decision-makers and managers with the information needed to plan permanent upgrades to security programs and to identify the necessary resources for protecting sensitive assets, including special nuclear material.

In 2003, the Secretary of Energy emphasized the need to maximize the use of innovative security technologies to meet the DBT requirements. Based on the importance of securing special nuclear materials and the Secretary's emphasis on deploying innovative technologies, we conducted this audit to determine whether the Department's National Nuclear Security Administration (NNSA) had made progress in deploying innovative security technologies to meet security requirements.

RESULTS OF AUDIT

NNSA made significant progress in deploying innovative technologies to meet the DBT requirements. Specifically, six NNSA sites that possessed special nuclear materials deployed 75 technology upgrades by the end of Fiscal Year 2006 at a cost of about $63 million. While progress had been made by NNSA sites in deploying technologies, a few technologies had not performed as expected and some maintenance requirements were more than anticipated by NNSA sites. For example, sites which had deployed infrared radar systems incurred annual maintenance costs that were nearly as much as the purchase price.

NNSA sites did not always analyze and evaluate technologies under actual operating conditions before selecting them for deployment. Specifically, NNSA sites did not have key performance and maintenance requirements data that was validated for actual site operating conditions to use in the selection of technologies. Rather, the sites used data from other sources, such as the military and commercial vendors that was not based on their operating conditions. For example, the performance data used to select the infrared radar systems was obtained from the vendors and the military. This data, however, was not based on the 24 hours a day/7 days a week operating conditions at NNSA sites. As a result, some of the selected technologies were not as reliable as expected and some maintenance requirements were greater than the sites anticipated.

Site officials had limited time to identify and select technologies before procuring and installing upgrades by the end of Fiscal Year 2006, as required by the Department. Further, NNSA told us that in the past they had used validated performance data that had been developed by Sandia National Laboratories. However, Sandia's validation of performance data was unavailable due to budget constraints.

During the audit, the Department and NNSA took steps to improve the availability of technology performance and maintenance data. We made further suggestions regarding the use of validated performance data in the selection of security technologies.